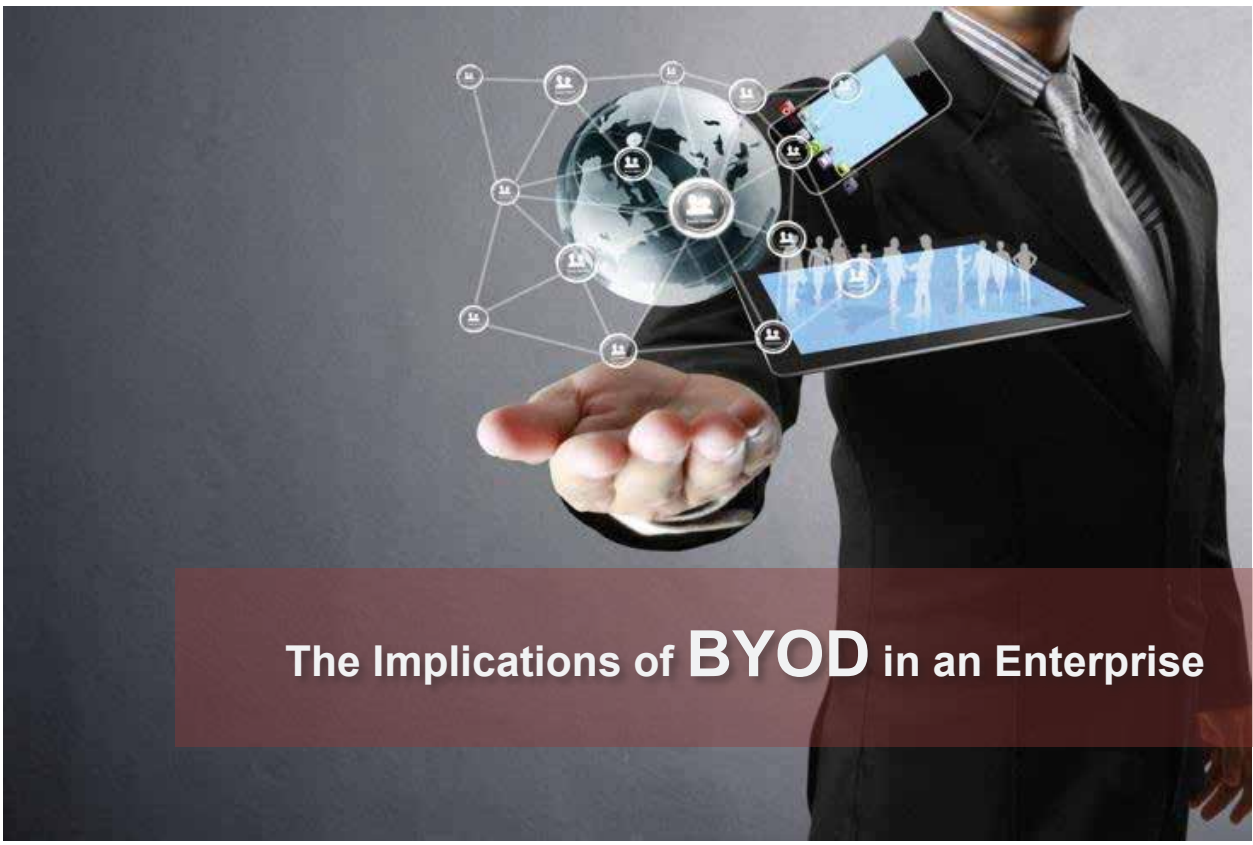
Ideas to Solutions



Abstract

Bring Your Own Device is a consumer led trend in the IT sphere, which has been doing the rounds in all industry verticals in the recent times. The term BYOD, coined by marketers to pronounce IT consumerization, is leading companies to tread on a fine line between their IT policies and employee engagement. The continuously growing demand of employees for anytime, anywhere access and the easy availability of high performance personal devices is driving this trend to the point that companies have no other option but to accept it.

BYOD is a trend, massively fuelled by the rapid influx of personal smartphones, tablets and laptops and other devices in the corporate domain. The phenomenon is altering the way IT organizations and users address network access security. From an enterprise point of view, BYOD means offering support to 'n' number of different devices with different OS, while simultaneously maintaining security, integrity and low costs. On the other hand BYOD from user's point of view means using his/her personal device to suit both personal as well as work related issues.

This paper discusses the benefits and considerations associated with BYOD, its implications and how organizations can implement it effectively. This white paper is not meant to be comprehensive, but rather focus on key areas for consideration and examples of existing policies and best practices in addition to providing an overview of considerations for implementing BYOD.

Introduction

Consumers today are more tech savvy than they were before, have an ownership of multiple devices and are adept at operating the latest technologies. Further, the roaring popularity and consumption of social media today means no one is away from their smartphone, tablet or laptop. High end and high performance devices are becoming the norm today, with every user owning at the least one high performance device either for work or for personal use. Additionally, with the advent of technologies such as POP mail on mobile devices, support for enterprise applications and quad-core processing power, it was only a matter of time that such personal devices invaded the corporate workspace.

In this context, Bring Your Own Device (BYOD) is a consumer-led trend that is revolutionizing the 21st century enterprise workspace, that enables employees to work from anywhere in the globe at any time and on any device either within the conventional workspace or outside. This is a trend that has been under way for quite some time, but grew faster since smart phones and tab PC's were introduced.

For some, BYOD is a natural progression as the fine line between work and personal life fades away. The omnipresence of email on the phone today does not mean work ends at the conventional time, but new work timings are defined. Add to it, technologies such as 4G LTE, Wi-Fi, remote access technology and others, working from home or on the way to office are becoming normal. Further, with the consumerization of enterprise mobility, a growing percentage of workers are using their personal devices to access corporate resources and thereby fanning the BYOD trend.

Understanding BYOD

Humble Beginnings

BYOD has its roots in the early 80s and 90s when affordable computing devices and technologies were gaining popularity; all driven by Microsoft powered PCs. The popularity of such devices had for the first time made organizations reconsider the use of non-corporate devices for work and accept the fact that work could be done beyond the traditional workspace. The advent of portable computers further consolidated the fact as work could now be completed without being present at the office in a timely manner. However, the use of such devices for work remained limited due to the nascency of Internet and issues related to security and command.

Today, with advancements in almost every sphere of Internet, consumer technology and mobile applications, BYOD has become the most commonly used word or acronym in the enterprise space. Devices today are more powerful than ever, with a new device, replete with its own features, an increasingly sophisticated OS coming out in the market every month. Once simply a means communications, these devices are now capable of running powerful enterprise apps, churning out HD video and consuming ever more bandwidth. These devices have reached such level of maturity today that they can easily replace clumsy equipment once thought key to businesses and render them obsolete at one go.

In this context, BYOD is the Holy Grail that not only promises and enables companies to become more agile and customer-focused, but also ensures employees rapidly create, apply and consume knowledge at work, thereby deriving the much sought competitive advantage in a knowledge-driven economy. However, organizations still face security and data challenges in incorporating such devices in their IT environments.

Current State of Affairs

With consumer electronics at its technical peak, the market today is always abuzz with a new product being launched which is better than the last. Today users from the CEO down to newly hired interns want the ability to use personal devices for work. This is all drawn from the belief that personal devices are more powerful, flexible, and usable than those made available by corporate.

A Necessity Today or a Passing Trend?

BYOD has had its fair share of believers, who believe it is a fact no IT organization can dodge, while naysayers believe BYOD is just a passing fad. No matter what the fate of BYOD is in the long run, current scenarios are very much aligned towards the implementation of BYOD.

According to a Forrester research report of 2011, 60% of companies already allow their employees to use personal devices for work[1]. Additionally, Gartner, another leading IT research organization, states that 50 percent of employees use personal devices for work in one form or the other. "By 2014, 90 percent of organizations will support corporate applications on personal devices"[2], predicts, Gartner. From the above mentioned statistical analysis, one can easily conclude that BYOD is here to stay no matter what other complexities prevail.

However, in total contrast to the reports from Gartner and Forrester, Nucleus Research, another leading research firm, believes BYOD will in fact decline in the year 2013, as companies start focusing on the high total cost of ownership with no apparent ROI.[3] However; it is too early to decide on the fate of BYOD as the viewpoints range far and wide.

Considering the current industry trends, organizations are already starting to change existing IT policies to assimilate BYOD policies. There are a number of reasons which add up to BYOD. The first being the immi nent expiration of Windows XP support, which has been doing the rounds in IT circles for some time now. This has been a major driver for IT organizations to assess substitute desktop strategies, as a result making them align with BYOD. The other major reason driving BYOD is mass consumption of high performance mobile devices which are powerful than most of the conventional corporate work equipment. Advancements in Internet and cloud services are other drivers of BYOD.

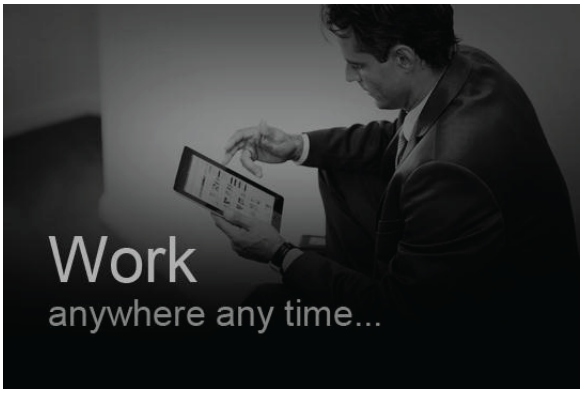
Further, BYOD has become such a popular trend due to the fact that each corporation can develop a model tailored to their unique business and employee needs.

Key Impact Areas

The implementation of BYOD has far reaching repercussions, both of advantageous and disadvantageous in nature. A major driver of BYOD implementation is productivity, which stems from employee satisfaction and mobility, as well as low technology costs. On the flip side, the surge in BYOD has IT departments scrambling to make sure that networks can accommodate numerous devices securely. In order to understand the key impact areas of BYOD, its benefits and drawbacks from the point of view of an enterprise need to be identified.

Benefits of BYOD

Following are the marked benefits that BYOD can offer enterprises:



Management and work flexibility

As BYOD encourages the utilization of devices of employees, the added burden of selecting and managing a plan and a service provider on the part of an organization is eliminated. Further, organizations also do not need to monitor the telecom usage, data usage of employees for overages or other extras. Further, if employees are able to work from home, on the road or in the workplace, there are obvious benefits. With a well-managed BYOD infrastructure, employees can easily juggle their family, social and work lives while maintaining a high level of productivity.

Cost savings

By implementing BYOD, enterprises can save money not only from overhead costs in managing a corporate phone plan but also from individually-managed call, data, and SMS plans, which are much more cheaper than those available for enterprises. In short, BYOD shift costs of the employer to the employee. With the employee paying for most or all of the costs of the hardware, voice or data services, organizations can save a lot of money.

Enhanced employee productivity and satisfaction

People purchase laptops and smartphones according to their preferences, carefully scrutinizing each and every feature, running checks and cross checks with other models in the market. These devices are the devices they prefer and like as they invest in them. So it is logical that these people will use their own devices rather than using devices running legacy or almost obsolete hardware and software. It is seen that employees are likely to perform productively if the devices they are working with offer a sense of familiarity and comfortability.

Faster utilization of new technologies

Previously it was enterprises, which used to offer employees access to new as well as cutting edge developments in technology. However, with changing market dynamics, it is now the employees who get first hand access to such technologies. Enterprise need to strike deals to avail new technologies and are sometimes bound by existing deals, which bind the enterprise to a technology for a period of time. But the scenario is completely different from an employee point of view. An employee does not have to abide by a contract to avail and consume a new technology. With BYOD, the uncertainty is further mitigated as an employee can readily purchase and avail the latest technology and dump it without any thought in case of obsolescence. In the context of BYOD, this ultimately means that business will gain faster access to new technology. The latest technical features and tools will be utilized by the employee, therefore utilized by the company.

In addition to the above mentioned benefits, benefits such as enhanced employee contentment, freedom of choosing any type of device, convenience of using a single device instead of multiple devices are popularizing BYOD. Another relatively unusual benefit that BYOD brings to an enterprise is the ability to attract prospective employees as employees find the ability to bring their own device into the workplace appealing.

Drawbacks of BYOD

The availability of innumerable smart mobile and computing devices in a BYOD environment not only creates complexities but also overwhelms the infrastructure set up by a normal or even the most sophisticated and technically advanced organizations. Further, with limited control over the vast choice of devices, organizations face significant challenges in protecting data, ensuring security, providing support, complying with regulations and minimizing IT infrastructure costs. With smart phones and laptops replacing traditional desktop workstations driven by BYOD, data can easily move in and out of the company breaching security and leaking confidential information.

Following are the major areas of concern or in other words drawbacks of BYOD:

Costs

BYOD is a radical movement, which calls for out of box implementation solutions. BYOD no doubt can help organizations minimize costs but the potential to save money depends on how well organizations understand the requisite expenditure associated with BYOD. Unnecessary BYOD outlays, such as mobile expense compensations, investments in solutions supporting heterogeneous devices

and customizing apps to run on multiple platforms, inflate expenses not minimize them.

Content Monitoring and Management

Both wired and wireless networks have today evolved to become an indispensable and mission critical part of every organization's IT infrastructure. However, with the advent of trends like BYOD and its acceptance amongst employees, organizations are having a tough time negotiating the challenges posed by this radical movement. As employees start to bring their personal devices to the workspace, controlling and ensuring performance and security of the network has become a key challenge. The absence of tools and visibility to effectively monitor networks with such heterogeneity is only worsening the situation.

Updates and Support

The heterogeneity in the device landscape makes it challenging to develop and implement appropriate security measures as well as design a uniform platform, where an iOS device seamlessly talks to an Android device. Further, with BYOD an organization can no longer standardize a single device, and instead needs to prepare itself for supporting a broad range of devices across multiple platforms. For instance, if an organization intends to update its internal services available via a web service, it can't just target a device of a particular make. It has to ensure that the services will work with all of its employee's devices. Additionally, providing support for the numerous devices used by employees, while ensuring reductions in overall support costs, is a major implementation challenge on the part of organizations.

Data Insecurity

Using personal devices for work no doubt has many benefits but what employees fail to comprehend is the data security concerns it raises. In comparison to most corporate hardware, no matter how obsolete they are, it is seen that employee owned devices are more prone to malware attacks, theft and loss, all because of their sensitive nature, perceived monetary value and portability. Further, mixing personal and business applications and data has the potential to introduce malware that can infect devices and ultimately lead to the compromise of corporate data. Additionally, tracking a lost device and wiping off sensitive company data may sound easy but is arduous tasks as both involve radical advancements in technology.

Compliance

Compliance mandates such as HIPAA, PCI DSS and GLBA are particular about safeguarding data, irrespective of the device on which data is stored. In the event of data breaches, organizations end up paying heavy fines. Further, if an organization is into developing security-related software and goes after some kinds of certification (like EAL 2+ levels) then the development environment is taken into account. The presence of uncontrolled machines in that environment may impair the certification process. To state things plainly, it is pretty difficult to guarantee that no backdoor was inserted in the code of an application when the developers' machines are outside of reach of any security policy.

Employee vs. IT Department story

In short the BYOD story in an enterprise can be summarized as follows:

Why IT Dept. hates BYOD?	Why employees love BYOD?
❖ Increased Distraction	❖ Increased Productivity
❖ Higher Costs	❖ Lowered Cost
❖ Increased Risk	❖ Increased Freedom
❖ More systems to deal with	❖ Quicker Access to the tools they use
❖ More Administration	❖ Less Administration

Considerations for IT Organizations

Considering the implications of BYOD, its implementation in an enterprise needs to be an iterative process. Organizations should first emphasize on building support for enterprise technologies like email and collaboration systems, which can help them lay the basis for expansion to more varied mission-specific applications and enterprise offerings.

BYOD, being a relatively new and radical trend, entails out of the box thinking on the part of both companies and employees. New approaches for security, new ways of managing applications, and novel technical support processes need to be thought of and properly evaluated in this context. Further, the business case for implementing BYOD varies from one organization to the other, but primarily involves the following key drivers:

- **minimizing costs**
- **increasing program productivity and effectiveness,**
- **adapting to a changing workforce,**
- **enhancing user experience**
- **implementing new technologies**

Before implementing BYOD organizations need to devise a strategic policy carefully outlining –which devices and operating systems to support, assess security requirements, define availability as per employee role and designation and the extent of risks they are willing of take in case of breach. In this context, the following points need to be clearly defined:

Business goals

Before implementing BYOD, an organization should have a clear understanding of its business goals and accordingly decide how many employees will participate in the BYOD

program and then allocate the capital and operational expenses, and the support costs. An organization should also carefully evaluate if it wants to pay for some part or all of the cost of employees' mobile devices or service plans. Building such an understanding in BYOD context helps the organization in deciding an appropriate return on investment model.

Risk Tolerance

Organizations should be ready to embrace the pitfalls associated with BYOD and accurately assess the requirements for data protection. This has special meaning in highly sensitive environments where there may be legal or compliance issues or special protection for senior executives' communications.

An organization should carefully factor in its risk tolerance capabilities as risk varies by industry and geography. For instance, healthcare providers and financial services firms generally have tighter legal and compliance requirements than universities and colleges.

Differentiation between personal and organizational intellectual property

BYOD involves use of personal devices; however, organizations should note that putting restrictions on such devices in the same way as that of conventional corporate devices is out of question. Organizations should be able to separate and segregate personal and company information successfully, without infringing upon the personal space of an employee. This will allow organizations to remove business applications and data if the employee leaves the organization, without affecting the person's photos and applications.

Utilization of Mobile Device Management Solutions

Organizations should proactively implement Mobile Device Management (MDM) solutions while defining a BYOD infrastructure in an enterprise. MDM solutions are capable of ensuring the ability to remotely lock or wipe lost or stolen mobile devices. Further, MDM solutions typically allow for over-the-air distribution of applications, data and configurations, which simplifies managing a large number of mobile devices, whether company-owned or employee-owned.

Conclusion

BYOD is here to stay and is becoming more prevalent day by day as more and more companies start implementing it. It is a radical trend that guarantees employees the freedom to work on their own devices simultaneously relieving IT of significant financial and management burdens. BYOD is all about allowing employees to do their jobs and be as productive as possible—which is why it is finding such wide scale acceptance. But it should be noted that **BYOD will never be able to deliver on the promises of streamlined management and cost savings without a well-written policy and a robust management platform.**

References:

- [1] Forrester Research, Inc., Forrsights: Mobility Dominates Enterprise Telecom Trends In 2011, July 22, 2011.
- [2] http://www.gartner.com/it/page.jsp?id=1480514
- [3] http://nucleusresearch.com/news/press-releases/nucleus-research-announces-top-predictions-for-tech-trends-in-2013/

About Xavient Digital, powered by TELUS International

- Headquartered in Simi Valley, CA, Xavient Digital, powered by TELUS International (Formerly Xavient Information Systems),is a leading provider of global IT and engineering services and solutions. Since its inception in 2002, Xavient has grown to be a tier-one IT Professional Services and Solutions provider for telecommunication, broadcasting, manufacturing, retail, and healthcare companies.
- It is the preferred transformation partner across product and vendor evaluation; business process re-engineering; outsourcing and off-shoring; product implementation; custom solution development and IT professional services for several Fortune 1000 companies.
- Xavient leverages its proven expertise in Global Delivery Models with centers of excellence in Application Development, QA & Testing, Managed IT Infrastructure services and IT Application & Production environment.

Our Locations

Corporate Location

CALIFORNIA
2125, Suite. B, Madera Rd
Simi Valley, CA 93065
Main Line: 1.805.955.4111
Fax Line: 1.805.955.4144

GEORGIA
2 Ravinia Drive
Suite 500
Atlanta, GA 30346
Main Line: 1.678.801.9966

COLORADO
9800, Mount Pyramid Court
Suite 400
Englewood, CO 80112
Main Line: 1.303.900.0700

WASHINGTON
800, Bellevue Way NE
Suite 400
Bellevue, WA 98004
Main Line: 1.425.442.6629

NOIDA
54, E15, 21, 24 NSEZ, Phase II
Noida – 201305, U.P. (India)
Main Line: 91.120.4743000,
91.120.4532000
Fax No: 91.120.4240948

CANADA
2 Robert Speck Parkway
Suite 750, Mississauga ON
L4Z 1H8
Phone: 1.905.361.9816

VIRGINIA
13800 Coppermine Rd,
Herndon, VA 20171

For further information please write to : info@xavient.com